1 (a) **Lema:** Če k ni alg. zaprt, potem za vsak $n \in \mathbb{N}$ obstaja $f \in k[X_1, \dots, X_n]$, katerega edina ničla je $(0, 0, \dots, 0) \in k^n$.

Dokaz: Obstaja $F(X)$, ki v k nima ničle; npr.

$$F(X) = a_m X^m + \dots + a_1 X + a_0 .$$

Trditev bomo dokazali z indukcijo. Za $n=1$ vzamemo kar $f(X_1) = X_1$. Sicer pa "homogeniziramo" F; $F\left(\frac{X}{Y}\right)$ pomnožimo z najmanjšo potenco Y, da dobimo polinom v dveh spremenljivkah X in Y:

$$Y^m F\left(\tfrac{X}{Y}\right) = a_m X^m + \dots + a_1 X Y^{m-1} + a_0 Y^m .$$

Očitno je $Y^m F\left(\frac{X}{Y}\right) = 0 \iff X = Y = 0$. S tem smo dokazali trditev za $n=2$. Podobno za $n>2$. Če je $f_0 \in k[X_1, \dots, X_{n-1}]$ polinom, katerega edina ničla je $(0, \dots, 0) \in k^{n-1}$. Ponovno homogeniziramo in množimo z ustrezno potenco

$$f := X_n^u \cdot f_0\left(\frac{X_1}{X_n}, \dots, \frac{X_{n-1}}{X_n}\right).$$

Če $X_n \neq 0$, potem je $f(X_1, \dots, X_n) = f_0\left(\frac{X_1}{X_n}, \dots, \frac{X_1}{X_n}\right) \cdot X_n^u \neq 0$. Če pa je $X_n = 0$, je $f = f_0(X_1, \dots, X_{n-1})$ in je enak 0 natanko tedaj, ko je $X_1 = \dots = X_{n-1} = 0$. ■

Če je sedaj $V = \{f_1(\underline{x}) = \dots = f_k(\underline{x}) = 0\}$,

je $V = \{\underline{x} \mid f(f_1(\underline{x}), \dots, f_k(\underline{x})) = 0\}$,

kjer je f iz zgornje leme.

(c) Naj bo npr. $k = \mathbb{C}$ in si oglejmo alg. množico $(0,0) \in \mathbb{C}^2$. Denimo, da obstaja $f \in \mathbb{C}[X, Y]$, katerega edina ničla je $(0,0)$:

$$f = \sum_{m=0}^{s} \sum_{n=0}^{r_m} \alpha_{mn} Y^n X^m .$$

Ker je $\mathbb{C}$ alg. zaprt obseg, za vsak m in vsak $\beta \in \mathbb{C}$ velja $\sum_{n=0}^{r_m} \alpha_{mn} \beta^n = 0$. V posebnem za vse $\beta_0, \beta_1, \dots \beta_{r_m} \in \mathbb{C}$

$$\begin{bmatrix} 1 & \beta_0 & \cdots & \beta_0^{r_m} \\ \vdots & & \ddots & \vdots \\ 1 & \beta_{r_m} & \cdots & \beta_{r_m}^{r_m} \end{bmatrix} \begin{bmatrix} \alpha_{m0} \\ \vdots \\ \alpha_{m r_m} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Če $\beta_i \in \mathbb{C}$ izberemo sedaj tako, da je transcendenten nad $\mathbb{Q}(\beta_0, \dots, \beta_{i-1})$, potem je matrika na levi obrnljiva. Sledi $\forall m \, \forall i \;\; \alpha_{mi} = 0$. Protislovje.

Za drugi del naloge naj bo V poljubna neskončna podmnožica k, ki ni cel k (k je lahko poljuben neskončen obseg). Če ima nek polinom neskončno različnih ničel in je polinom 1 spr, potem je identično enak 0. Torej V ni algebraična množica. ■

(b) Vsaka končna množica je algebraična.

Končen obseg ni nikoli alg. zaprt:

če je npr. $k = \{a_1, \dots, a_r\}$, potem polinom

$$(X - a_1) \cdots (X - a_r) + 1$$

v k nima ničle.

Torej (b) sledi iz (a).

(2) Pokazali bomo, da je preslikava

$$\begin{aligned} \Phi : k(\mathcal{S}) &\longrightarrow k(V_1) \times \cdots \times k(V_n) \\ [U, r] &\longmapsto \big([U \cap V_1, r|_{V_1}], \ldots, [U \cap V_n, r|_{V_n}]\big) \end{aligned}$$

izomorfizem algeber. Naj bo (U, r) regularna funkcija. Tedaj je $U \cap V_i$ odprta gosta množica v varieteti V_i. Inkluzija $V_i \hookrightarrow \mathcal{S}$ inducira surjektivni morfizem $k[\mathcal{S}] \to [V_i]$. Vzemimo poljuben $x \in U \cap V_i$. V okolici x je $r = \frac{f}{g}$ za funkciji $f, g \in k[\mathcal{S}]$. Potem v okolici točke x v množici V_i velja $r = \frac{\bar{f}}{\bar{g}}$, kjer je $\bar{h}$ slika polinomske preslikave h pri epimorfizmu $k[\mathcal{S}] \to [V_i]$. Torej je $r|_{\mathcal{S} \cap V_i}$ regularna na $\mathcal{S} \cap V_i$. Z $[U \cap V_i, r|_{V_i}]$ označimo pripadajočo racionalno funkcijo (to je v bistvu razširitev $r|_{\mathcal{S} \cap V_i}$). S tem smo dokazali, da je preslikava Φ dobro definirana. Očitno pa je homomorfizem algeber.

Sedaj bomo poiskali inverzno preslikavo preslikave Φ. Vzemimo poljuben $([U_1, r_1], \ldots, [U_n, r_n]) \in \times_{i=1}^{n} k(V_i)$. Za vsak j naj bo $\widehat{r}_j$ zožitev r_j na komplement $\widehat{U}_j$ množice $V_j \cap (\cup_{i \neq j} V_i)$ v definicijskem območjo funkcije r_j. Za vsak j je $\widehat{U}_j$ odprta gosta množica v V_j in $U_j \cap U_i = \varnothing$ za $i \neq j$. Funkcije $\widehat{r}_j$ definirajo regularno funkcijo na odprti gosti množici $\cup_{j=1}^{n} \widehat{U}_j \subseteq \mathcal{S}$. Naj bo $[U, r]$ racionalna funkcija, ki jo določajo te funkcije. Iz principa identičnosti takoj sledi, da je preslikava $([U_1, r_1], \ldots, [U_n, r_n]) \longmapsto [U, r]$ inverz preslikave Φ. $\square$

3 (a) Očitno je družina konstr. množic zaprta za končne unije in preseke ter komplemente. Vsaka alg. množica je konstruktibilna. Ker pa je vsaka bazična konstr. mn. oblike $\langle F_1 = \cdots = F_r = 0;\ G_1 \neq 0, \ldots, G_s \neq 0 \rangle =$

$$= \langle F_1 = 0 \rangle \cap \cdots \cap \langle F_r = 0 \rangle \cap \Big(\langle G_1 = 0 \rangle \cup \cdots \cup \langle G_s = 0 \rangle \Big)^c,$$

je to najmanjša družina s temi lastnostmi.

Alg. podmnožice v k so ntk. končne množice, $\emptyset$ in k. Torej so konstr. mn v k ntk.: $\emptyset$, k, končne in kokončne (tj. komplementi končnih) množice.

(b) Naj bo $V = \{ \underline{x} \in k^n \mid F_1(\underline{x}) = \cdots = F_r(\underline{x}) = 0,\ G_1(\underline{x}) \neq 0, \ldots, G_s(\underline{x}) \neq 0 \}$ konstr. množica. Potem je V projekcija alg množice

$$Z = \{ (x, y) \in k^{n+s} \mid F_1(\underline{x}) = \cdots = F_r(\underline{x}) = 0,\ y_1 \cdot G_1(\underline{x}) = 1, \ldots, y_s \cdot G_s(\underline{x}) = 0 \}$$

vzdolž zadnjih s komponent.

Projekcija alg. množice ni nujno algebraična množica:

$$Y = \{ (x, y) \in k^2 \mid xy - 1 = 0 \}$$

$Z :=$ projekcija vzdolž druge komponente

$$= \{ x \in k \mid \exists y \in k \quad xy = 1 \} =$$

$$= k \setminus \{0\}$$

Če je sedaj obseg k npr. $\mathbb{C}$, potem je vsak polinom, ki uniči $\mathbb{C} \setminus \{0\}$, identično enak 0.

Torej Z ni algebraična množica.

(d) $\varphi : V_1 \to V_2$ konstruktibilna, $S \subseteq V_1$ konstr.

Potem je $\varphi(S)$ projekcija množice $\Gamma_\varphi \cap (S \times V_2)$, ki je očitno konstruktibilna. Torej je tudi $\varphi(S)$ konstruktibilna množica po Chevalleyevem izreku.

(c) Naj bo $Z = \{ \underline{x} = (x_1, \ldots, x_n) \in k^n \mid F(\underline{x}) = 0 \}$ za nek $F \in k[X_1, \ldots, X_n]$. S $\pi_n : k^n \to k^{n-1}$ označimo proj. vzdolž zadnje koord. F zapišemo kot polinom v X_n:

$$F(x_1, \ldots, x_{n-1}, X_n) = F_0(x_1, \ldots, x_{n-1}) X^0 + \cdots + F_r(x_1, \ldots, x_{n-1}) X^r$$

Očitno je $\pi_n(Z) = \{ y = (y_1, \ldots, y_{n-1}) \in k^{n-1} \mid \exists y_n \in k\ F(y, y_n) = 0 \}$

Ker je k alg. zaprt, ima pri fiksnem y polinom $F(y, \cdot)$ ničlo v k ntk tedaj, ko velja

$$F_0(y) = 0 \ \vee\ (F_0(y) \neq 0 \wedge F_1(y) \neq 0) \vee \cdots \vee (F_0(y) \neq 0 \wedge F_r(y) \neq 0).$$

Torej je $\pi_n(Z) = \{ y \in k^{n-1} \mid F_0(y) = 0 \} \cup \{ y \mid F_0(y) \neq 0 \neq F_1(y) \} \cup \cdots \cup \{ y \mid F_0(y) \neq 0 \neq F_r(y) \}.$

Če pa je $Z = \{ \underline{x} \mid F(\underline{x}) \neq 0 \}$, potem je

$$\pi_n(Z) = \{ y \mid F_0(y) \neq 0,\ F_1(y) = \cdots = F_r(y) = 0 \}.$$

(e) Za prvi del bomo dokazali več: vsaka regularna presl. $r : V \to W$ je konstr. Naj bo U odp. gosta $\subseteq V$, kjer je r def. Tedaj je $\Gamma_r = \{ (\underline{x}, y) \mid y = r(\underline{x}) \} =$

$$= \{ (\underline{x}, y) \mid g_1(\underline{x}) \neq 0, \ldots, g_r(\underline{x}) \neq 0,\ y_1 = \tfrac{f_1}{g_1}(\underline{x}), \ldots, y_r = \tfrac{f_r}{g_r}(\underline{x}) \},$$

kjer je $r = \left(\frac{f_1}{g_1}, \ldots, \frac{f_r}{g_r} \right)$ na U. Ta množica pa je očitno konstruktibilna. Obrat <u>ne</u> velja: obstajajo konstruktibilne preslikave, ki niso racionalne.

Vzamemo lahko npr. $\mathbb{C} \xrightarrow{\varphi} \mathbb{C}$, $x \longmapsto \begin{cases} \frac{1}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$.

Kratek premislek pokaže, da φ ni racionalna. ■

$\boxed{4}$ (a) Ker je $\sqrt{m}$ celosten nad $\mathbb{Z}$, iščemo cel. zaprtje $\mathbb{Z}$ v $\mathbb{Q}[\sqrt{m}]$. Naj bo to R. Vsak $\alpha \in R$ je stopnje ≤ 2 nad $\mathbb{Q}$. Torej za vsak $\alpha \in R$ obstaja polinom stopnje 2 nad $\mathbb{Z}$, ki uniči α. $a+\sqrt{m}\cdot b$

Ker velja $\alpha^2 - 2a\alpha + (a^2 - mb^2) = 0$, je elt oblike $a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ element kolobarja R natk tedaj, ko $2a \in \mathbb{Z}$ in $a^2 - mb^2 \in \mathbb{Z}$. Po opazki iz prvega stavka smemo predpostaviti, da je razcep m-ja brez kvadratov.

Če je $\alpha \in R$, je $2a \in \mathbb{Z}$. Ker je R kolobar in vsebuje $\mathbb{Z}$, smemo predpostaviti $2a \in \{0, 1\}$. Torej $a \in \{0, \frac{1}{2}\}$.

$a=0$: Velja še $b^2 m \in \mathbb{Z}$ in zato (ker m ni deljiv s kvadrati) $b \in \mathbb{Z}$. Sledi $\alpha \in \mathbb{Z}[\sqrt{m}]$.

$a=\frac{1}{2}$: Velja $\frac{1}{4} - mb^2 \in \mathbb{Z}$; $\frac{1}{4}(1 - (2b)^2 m) \in \mathbb{Z}$. Kot zgoraj, $2b \in \mathbb{Z}$ in spet b.š.s. $b \in \{0, \frac{1}{2}\}$. Če je $b = 0$, potem $\frac{1}{4} \notin \mathbb{Z}$. Če je $b = \frac{1}{2}$, potem mora biti $\frac{1}{4} - \frac{m}{4} \in \mathbb{Z}$.

Torej:
$$R = \begin{cases} \mathbb{Z}[\sqrt{m}] & \mid m \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{m}] & \mid m \equiv 1 \pmod 4. \end{cases}$$
□

(b) Poiščimo najprej obseg ulomkov za
$$R := k[X,Y]/(Y^2 - X^3 - X^2).$$
Preslikava
$$\Phi : k[X,Y] \longrightarrow k(W)$$
$$X \longmapsto W^2 - 1$$
$$Y \longmapsto -W^3 + W$$
je homomorfizem k-algeber z jedrom $(Y^2 - X^3 - X^2)$, torej inducira vložitev $\varphi : R \longrightarrow k(W)$. Po drugi strani pa je $W = \varphi(-Y)\cdot\varphi(X)^{-1}$. Torej je $k(W)$ obseg ulomkov za R in φ vložitev. Očitno je $\varphi(R) \subseteq k[W] =: S$ in je S celostno zaprt, saj je polinomska algebra v 1 spremenljivki. Trdimo, da je S kar celostno zaprtje za R (oz. natančneje: za $\varphi(R)$). Vse, kar moramo dokazati, je to, da je S celostna razširitev od $\varphi(R)$. Vendar to takoj sledi, saj W uniči upr. polinom
$$Z^2 - 1 - \varphi(X) \in \varphi(R)[Z].$$
□

■